

Contenido

Visión global de la seguridad informática.....	2
Fiabilidad, confidencialidad, integridad y disponibilidad.....	2
Amenazas.....	3
Amenazas físicas.....	4
Amenazas lógicas.....	5
Amenazas según su origen.....	5
Amenazas según sus objetivos.....	6
Amenazas según la técnica empleada.....	6
Elementos vulnerables en el sistema informático.....	9
Análisis de vulnerabilidades del sistema.....	9
Seguridad física.....	12
Ubicación y protección física. Condiciones ambientales.....	12
Sistemas de alimentación ininterrumpida (SAI).....	13
Seguridad lógica.....	13
Políticas de almacenamiento.....	13
Medios de almacenamiento.....	14
Tipos de copias de seguridad.....	15
Recuperación del sistema.....	16
Recuperación de datos y borrado seguro.....	16
Criptografía.....	16
Criptografía de clave simétrica.....	17
Criptografía de clave asimétrica.....	18
Criptografía híbrida.....	19
Monedas digitales.....	19
Esteganografía.....	20
Sistemas de identificación.....	20
Sistemas biométricos.....	21
Firma digital.....	22
Auditorías de Seguridad Informática.....	25
Análisis forense.....	26

Visión global de la seguridad informática

La Seguridad Informática es la disciplina que involucra técnicas, aplicaciones y dispositivos que aseguran la autenticidad, integridad y privacidad de la información contenida dentro de un sistema informático, así como su transmisión.



Técnicamente resulta muy difícil desarrollar un sistema informático que garantice la completa seguridad de la información, sin embargo, el avance de la tecnología ha posibilitado la disposición de mejores medidas de seguridad para evitar daños y problemas que puedan ser aprovechados por los intrusos.

Se pueden hacer diversas clasificaciones de la seguridad informática en función de distintos criterios. Según el activo a proteger distinguiremos entre:

- Seguridad física: Controles externos al ordenador, que tratan de protegerlo contra amenazas de naturaleza física como incendios, inundaciones, etc.
- Seguridad lógica: Conjunto de medidas de seguridad y herramientas informáticas de control de acceso a los sistemas informáticos.

Según el momento preciso de la actuación distinguiremos entre:

- Seguridad pasiva: Se actúa después de producirse el percance, con lo que sólo se pueden minimizar los efectos ocasionados por el mismo (ejemplo tener copias de seguridad)
- Seguridad activa: Se actúa antes de producirse el percance, de tal manera que se evitan los daños en el sistema (ejemplo tener contraseñas seguras).

Para gestionar la seguridad es necesario realizar:

- Análisis de riesgos, investigar que posibles riesgos y valorar su impacto
- Gestión de riesgos, buscar medidas factibles para protegernos de estos riesgos
- Gobernanza, adaptar el funcionamiento de la empresa a estas medidas
- Vigilancia, observar continuamente que se aplican estas medidas y posibles nuevos riesgos
- Planificación de contingencia, como actuar ante un incidente de seguridad

Fiabilidad, confidencialidad, integridad y disponibilidad.

La fiabilidad se define como la probabilidad de que un bien funcione adecuadamente durante un período determinado bajo condiciones operativas específicas (por ejemplo, condiciones de presión, temperatura, velocidad, tensión o forma de una onda eléctrica, nivel de vibraciones, etc.).

Un sistema fiable debe tener entre otras: la capacidad de evitar fallos, tolerancia a defectos y capacidad de recuperación (tanto prestaciones como datos afectados).

La confidencialidad es la cualidad que debe poseer un documento o archivo para que este solo se entienda de manera comprensible o sea leído por la persona o sistema que esté autorizado.

La integridad es la cualidad que posee un documento o archivo que no ha sido alterado y que además permite comprobar que no se ha producido manipulación alguna en el documento original.

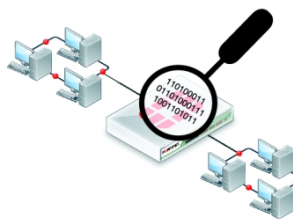
La disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

Amenazas

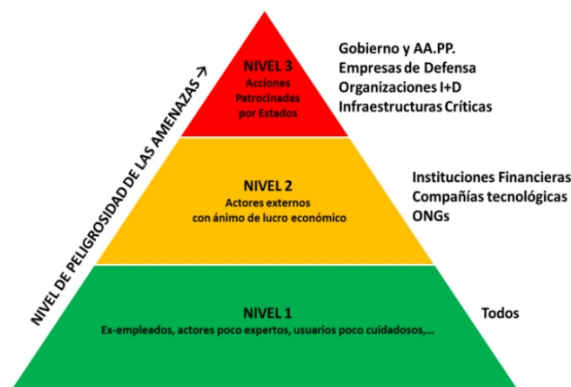
Entendemos por amenaza una acción que podría tener un efecto negativo sobre un activo (en su fiabilidad, integridad, confidencialidad o disponibilidad). Hay que tener en cuenta que una amenaza por sí misma no provoca un daño, pero podría provocarlo.

La mayoría de ataques a nuestro sistema provienen de personas que, intencionadamente o no, pueden causarnos enormes pérdidas. Los atacantes del sistema se pueden clasificar en:

- **Hackers:** son personas con grandes conocimientos informáticos y telemáticos que dedican un gran esfuerzo a investigar los sistemas operativos y los sistemas de seguridad para descubrir vulnerabilidades. La principal motivación de los hackers es seguir aprendiendo y mostrar las vulnerabilidades de los sistemas al mundo. En ningún caso buscan un beneficio económico o dañar la estructura del sistema. También son conocidos como hackers de sombrero blanco.
- **Crackers o hackers de sombrero negro:** el término hacker fue utilizado por los medios de comunicación de forma genérica, para referirse a cualquier intruso en un sistema, sin tener en cuenta la finalidad del ataque. La palabra cracker proviene de criminal hacker, es decir hackers criminales, hackers cuyas intenciones son maliciosas.
- **Phreakers:** son expertos en telefonía conocidos como los phone crackers, los crackers de la telefonía.
- **Ciberterroristas:** son expertos en informática y en intrusismo en la red, que ponen sus conocimientos al servicio de países y organizaciones para el espionaje o sabotaje informático.
- **Programadores de virus:** son expertos en programación, en sistemas y en redes, que crean pequeños programas dañinos.
- **Carders:** atacan los sistemas de tarjetas, especialmente los cajeros automáticos.
- **Sniffers:** son las personas que se dedican a escuchar el tráfico de la red, para intentar recomponer y descifrar los mensajes que circulan por la misma.
- **Script kiddie:** Son atacantes aficionados que no tienen conocimientos expertos y que usan herramientas automáticas de terceros que no entienden bien.



En cuanto a las amenazas, podemos hacer una primera clasificación en amenazas físicas y amenazas lógicas.



En el gráfico (Pirámide del daño ofrecida por el [Centro Nacional Criptográfico](#)) podemos observar el nivel de peligrosidad de las diferentes amenazas, estas han ido evolucionando y se han convertido en más sofisticadas y persistentes, es el nivel superior de la pirámide, lo que se denomina APT (Advanced Persistent Threats, amenazas persistentes y avanzadas) que son diseñadas por entidades con muchos recursos con el fin de obtener poder o grandes beneficios económicos.

Amenazas físicas

Las amenazas físicas afectan a las instalaciones y/o al hardware contenido en ellas y suponen el primer nivel de seguridad a proteger para garantizar la disponibilidad de los sistemas.

- Incendios. Se pueden evitar mediante la aplicación de los siguientes mecanismos de defensa:
 - El mobiliario de los centros de cálculo debe ser ignífugo.
 - Evitar la localización cerca de zonas donde haya sustancias inflamables.
 - Deben existir sistemas antincendios.
- Inundaciones. Podemos aplicar los siguientes mecanismos de defensa:
 - Evitar la ubicación de los centros de cálculo en las plantas bajas de los edificios para protegerse de la entrada de aguas superficiales.
 - Impermeabilizar las paredes y techos del CPD. Sellar las puertas para evitar la entrada de agua proveniente de las plantas superiores.
- Robos. Para evitarlos es necesario proteger los centros de cálculo mediante puertas con medidas biométricas, cámaras de seguridad, vigilantes jurados.
- Señales electromagnéticas. Podemos aplicar los siguientes mecanismos de defensa:
 - Evitar la ubicación de los centros de cálculo próximos a lugares con gran radiación de señales electromagnéticas.
 - En caso de no poder evitar la ubicación en estas zonas habrá que evitarlas en lo posible con uso de filtros, cableado especial, o si es posible, utilizar fibra óptica, que no es sensible a este tipo de interferencias.
- Apagones. Para evitar los apagones colocaremos Sistemas de Alimentación Ininterrumpida, SAI.
- Sobrecargas eléctricas. Hay SAI que incorporan filtros para evitar picos de tensión.
- Desastres naturales. La única forma de minimizar los riesgos es permaneciendo en continuo contacto con el Instituto Geográfico Nacional y la Agencia Estatal de Meteorología.

Amenazas lógicas

Bajo la etiqueta de amenazas lógicas encontramos todo tipo de programas que de una forma u otra pueden dañar a nuestro sistema, creados de forma intencionada para ello (software malicioso, también conocido como malware) o simplemente por error (bugs o agujeros).

Podemos clasificar las amenazas lógicas en función de varios criterios.

Amenazas según su origen

Teniendo en cuenta quién o qué las genera nos encontramos las siguientes amenazas:

- **Software incorrecto:** Las amenazas más habituales a un sistema provienen de errores cometidos de forma involuntaria por los programadores. A estos errores de programación se les denomina bugs, y a los programas utilizados para aprovechar uno de estos fallos y atacar al sistema, exploits.
- **Herramientas de seguridad:** Cualquier herramienta de seguridad representa un arma de doble filo porque de la misma forma que se utilizan para detectar y solucionar fallos también se pueden usar para encontrar vulnerabilidades del sistema.
- **Puertas traseras:** Software que permite el acceso al sistema de un usuario sin permiso. Durante el desarrollo de aplicaciones es habitual entre los programadores insertar 'atajos' en los sistemas habituales de autenticación del programa, a estos atajos se les denomina puertas traseras, y con ellos se consigue mayor velocidad a la hora de detectar y depurar fallos.
- **Bombas lógicas:** Software que permanece oculto hasta que se cumplen unas condiciones preprogramadas (por ejemplo una fecha), momento en el cual se ejecuta. Al ejecutarse puede borrar información, mostrar mensajes, etc.
- **Canales cubiertos:** Son canales de comunicación que permiten a un proceso transferir información de forma que viole la política de seguridad del sistema. Dicho de otra forma, un proceso transmite información a otros (locales o remotos) que no están autorizados a leer dicha información. Los canales cubiertos no son una amenaza demasiado habitual en redes de I+D.
- **Virus:** Un virus es una secuencia de código que se inserta en un fichero ejecutable (denominado huésped), de forma que cuando el archivo se ejecuta, el virus también lo hace, insertándose a sí mismo en otros programas. Algunas acciones que puede realizar un virus son:
 - Ralentizar o bloquear el ordenador.
 - Destruir la información almacenada en el disco.
 - Reducir el espacio en el disco.
 - Molestar cerrando ventanas, moviendo el ratón, mostrando mensajes, etc



Para evitar el ataque de este tipo de programas se han comercializado aplicaciones denominadas antivirus.

- **Gusanos:**



Los

que se propaguen por la red. Se diferencian en que éstos no necesitan la intervención del usuario ya que no se adjuntan a ningún programa sino que son distribuidos de manera completa por la red, consumiendo en la gran mayoría de los casos un gran ancho de banda de la red o

pueden llegar a bloquear el equipo infectado.

- **Troyanos:** O caballos de Troya son instrucciones escondidas en un programa de forma que éste parezca realizar las tareas que un usuario espera de él, pero que realmente ejecute funciones ocultas sin el conocimiento del usuario.
- **Spyware (spy –espia- y software).** Es un programa cuya misión es recopilar información del equipo infectado y enviarla a terceras personas para que puedan beneficiarse de esta.
- **Ransomware:** malware de rescate, es un tipo de malware que impide a los usuarios acceder a sus archivos y que exige el pago de un rescate para poder acceder. Actualmente suelen pedir un pago mediante criptomonedas. La versión más peligrosa es el ransomware de cifrado que encripta los ficheros.
- **Programa conejo o bacteria:** Bajo este nombre se conoce a los programas que no hacen nada útil, sino que simplemente se dedican a reproducirse hasta que el número de copias acaba con los recursos del sistema.
- **Técnicas salami:** Por técnica salami se conoce al robo automatizado de pequeñas cantidades de bienes (generalmente dinero) de una gran cantidad origen.

Amenazas según sus objetivos

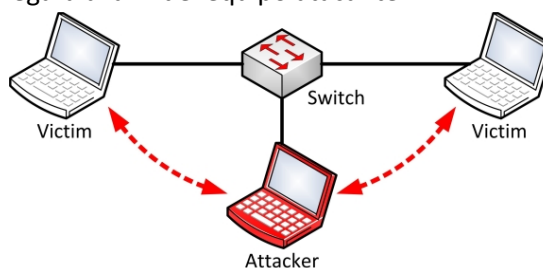
Según los objetivos de seguridad que vulneran nos encontramos las siguientes amenazas:

- **Interrupción,** este tipo de ataque vulnera la disponibilidad de un recurso del sistema o de la red. El recurso no podrá ser utilizado.
- **Intercepción,** ataca la confidencialidad. Un intruso accede a la información.
- **Modificación,** ataca la integridad. Los datos han sido manipulados por personal no autorizado en algún momento entre su creación y su llegada al destinatario.
- **Fabricación,** este tipo de ataque vulnera la autenticidad. Se trata de modificaciones destinadas a conseguir que el producto final sea similar al atacado de forma que sea difícil distinguirlo del original. Por ejemplo, el phishing.

Amenazas según la técnica empleada

También podemos clasificar los ataques en función de la técnica que se emplea:

- **ARP spoofing o suplantación de la identidad o ARP poisoning** aprovecha que el protocolo ARP fue diseñado de forma que las respuestas ARP reply se consideran 100% seguras, la técnica de spoofing (engaño o falseamiento) consiste en engañar a los equipos con respuestas ARP falsas, de esta forma el equipo apuntará a MAC erróneas que normalmente pertenecerán al atacante. Cualquier fichero que envíe el equipo del usuario atacado a cualquier otro equipo llegará a la IP del equipo atacante.
- **Man in the middle (hombre en medio)** se consigue utilizando la técnica



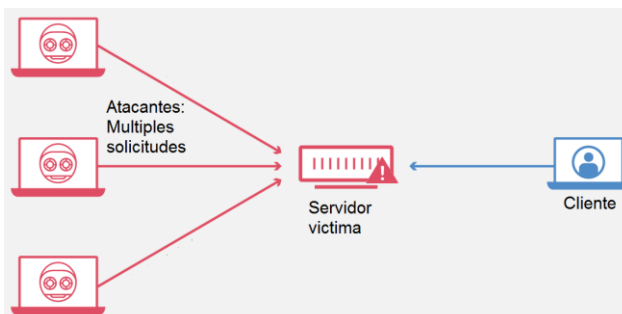
anterior de forma que un equipo atacante hace que le lleguen las comunicaciones entre los equipos víctimas, después las manipula y las envía a los equipos destinatarios. Este tipo de ataque también se puede realizar a niveles superiores.

- Server spoofing, dentro de estas suplantaciones tenemos por ejemplo DNS spoofing o engaño de DNS: Consiste en falsear la respuesta del servidor DNS sobre una petición y darle una dirección IP diferente a la real. Es decir, que cuando un PC atacado pide por ejemplo la IP de www.mibanco.es a su servidor DNS, el equipo atacante falseará el paquete de datos de los DNS con la respuesta y le puede engañar dándole la IP de otro equipo cualquiera. Así en vez de conectarse a su banco se conectaría a otra PC diferente pudiendo falsear la página de entrada de su banca electrónica y capturando sus claves de acceso a la misma.

<https://youtu.be/tlozZHUKXBc>

- Sniffing o análisis de tráfico: Este tipo de ataques consiste en escuchar el tráfico de la red. En las redes de área local que utilizan el hubs o concentradores que repiten toda la información recibida por cada uno de sus puertos. Si un equipo configura su tarjeta de red en modo “promiscuo”, podrá escuchar todo el tráfico de red, tanto los mensajes que van destinados a su IP como los que van destinados a otras IP. Para dificultar el uso de esta técnica, debemos sustituir los concentradores por switches o conmutadores, ya que estos últimos al usar tablas MAC sólo mandan la información recibida por el puerto adecuado. Aunque en los switches se puede usar MAC flooding, que consiste en saturar la memoria de los conmutadores para que pierdan la tabla de direccionamiento y terminen funcionando como concentradores, es decir, que reenvían la información recibida por todos los puertos por no saber por cuál de ellos debe enviarla.
- Conexión no autorizada a equipos y servidores: Este tipo de ataque consiste en descubrir distintos agujeros en la seguridad de un sistema informático y establecer con el mismo una conexión no autorizada.
- Malware: Es cualquier software o fragmento de código malintencionado, afectan a los sistemas con pretensiones como controlarlo o realizar acciones remotas, dejarlo inutilizable, reenvío de spam, etc. Entre los diferentes tipos de malware tenemos infeccioso como virus o gusanos, oculto como troyanos o backdoor, para obtener beneficios como spyware o ransomware, etc.

- Denegación del servicio (DoS): Este tipo de ataque se ejecuta contra servidores o redes de ordenadores con el propósito de interrumpir el servicio que están ofreciendo mediante el lanzamiento de grandes peticiones de servicio



simultáneas que provocan el bloqueo del servicio. Por ejemplo, un atacante envía peticiones DNS a un servidor DNS pero cambia su IP de origen por otro servidor, pongamos web, el servidor DNS responderá al servidor web, si además el atacante hace esta operación con muchos servidores DNS, esos inundarán de respuestas al

servidor web bloqueándolo. Este tipo de ataque se considera una de las principales amenazas de la actualidad

- Inundación de peticiones SYN: Más conocido por SYN Flood, consiste en hacer una petición de establecimiento de conexión a un servidor y no responder a su aceptación de conexión, esto provoca una saturación en las conexiones abiertas del servidor.
- Ataque por desbordamiento (overflow) aprovecha una vulnerabilidad del software que permite ejecutar código con los mismos permisos que la aplicación que presenta la vulnerabilidad y que utiliza un buffer en memoria, una vulnerabilidad puede ser no comprobar adecuadamente el tamaño de los parámetros que se pasan a la aplicación y que se escriben en ese buffer lo que pone a disposición del atacante acceder al buffer a través de estos parámetros y suele provocar una denegación de servicio por fallo en la aplicación.



social:

informática. Esta técnica consiste en obtener información secreta de una persona u organismo para utilizarla posteriormente con fines maliciosos.

confidencial del mismo suplantando la identidad de otras personas, organismos o páginas web de Internet. Uno de los métodos de phishing más utilizados hoy en día consiste en colgar en Internet una página que es copia idéntica de alguna otra



y solicitar a través de ellas credenciales de acceso. Para evitar estos ataques:

- Debemos mirar las direcciones URL de las páginas visitadas.
- Nunca entrar en la web de un banco a través de un enlace que recibimos por un correo electrónico.
- Introducir datos sólo en páginas web seguras. Mirar el certificado de autenticidad de la página web y que el protocolo que usa es https://.

Entre las versiones de phishing podemos encontrar el spear-phishing que adapta el phishing a cada individuo para ello se busca cualquier información de la empresa (nombres del personal, direcciones, etc) que permita personalizar el phishing.

Elementos vulnerables en el sistema informático

Entendemos por vulnerabilidad un fallo o debilidad que permite que se materialice una amenaza.

En un sistema informático lo que queremos proteger son sus activos, y que podemos agrupar:

- Hardware: Comprende todos los elementos físicos del sistema informático.
- Software: Comprende el conjunto de programas que se ejecutan sobre el hardware.

- Datos: Comprenden la información lógica que procesa el software haciendo uso del hardware. Es el activo más crítico, su pérdida puede suponer una catástrofe.

Análisis de vulnerabilidades del sistema

Existen diferentes vulnerabilidades que, dependiendo de sus características, las podemos clasificar e identificar en los siguientes tipos:

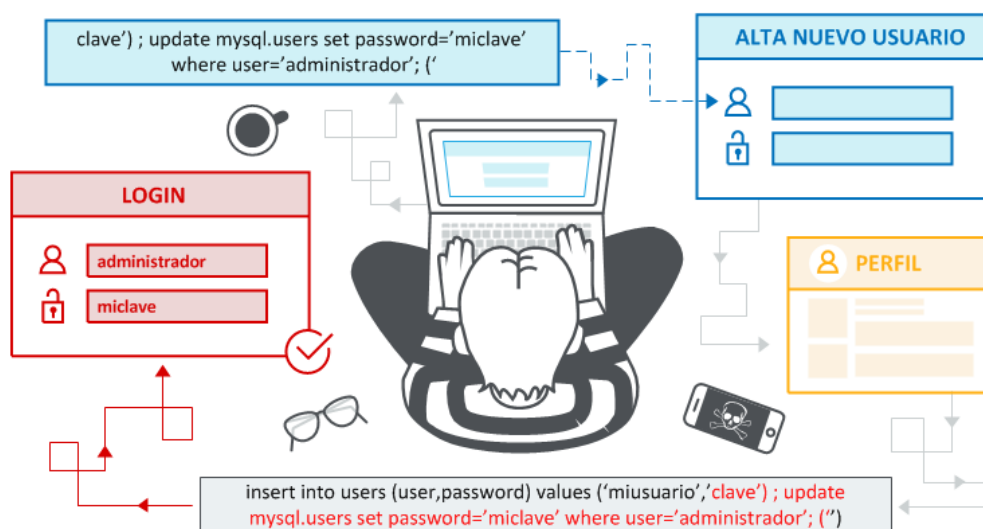
- De configuración: Es debida a cómo el usuario final configura el sistema. También se considera error de este tipo cuando la configuración por defecto del sistema es insegura, por ejemplo, una aplicación con usuarios por defecto.
- Validación de entrada: Este tipo de vulnerabilidad se produce cuando la entrada que procesa un sistema no es comprobada adecuadamente.
- Salto de directorio: Ésta aprovecha la falta de seguridad de un servicio de red para desplazarse por el árbol de directorios.
- Seguimiento de enlaces: Se producen cuando no existe una protección lo suficientemente robusta que evite el acceso a un directorio o archivo desde un enlace simbólico o acceso directo.
- Secuencias de comandos en sitios cruzados (XSS): Este tipo de vulnerabilidad abarca cualquier ataque que permita ejecutar código de script, como javascript, en el contexto de otro dominio. Por ejemplo, en un foro que permite insertar comentarios con un editor html, dentro del comentario se introduce un script: `<script>código malicioso</script>`, este código será ejecutado por todos los usuarios que accedan al foro y puede consistir en enviar datos comprometidos como cookies a un atacante.
- Inyección de comandos en el sistema operativo: Hablamos de este tipo de vulnerabilidad para referirnos a la capacidad de un usuario, que controla la entrada de comandos, para ejecutar instrucciones que puedan comprometer la integridad del sistema. Por ejemplo, supongamos un programa que realiza tareas mediante llamadas al sistema (por ejemplo que visualiza un fichero aprovechando el comando cat) y que recibe un parámetro, si al pasar el parámetro escribimos programa "fichero; rm -r /", si este programa está mal diseñado puede ejecutar un código no deseado (rm -r /)
- Inyección de código: Aquí encontramos distintos subtipos dentro de esta clase de vulnerabilidad:
 - Inyección directa de código estático: el software permite que las entradas sean introducidas directamente en un archivo de salida que se procese más adelante como código, un archivo de la biblioteca o una plantilla. En una inyección de código de tipo estático o también llamada permanente, una vez inyectado el código en una determinada parte de la aplicación web, este código queda almacenado en una base de datos. Una de las soluciones más apropiadas es asumir que toda la entrada es malévola. También es posible utilizar una combinación apropiada de listas negras y listas blancas para



asegurar que solamente las entradas válidas y previstas son procesadas por el sistema.

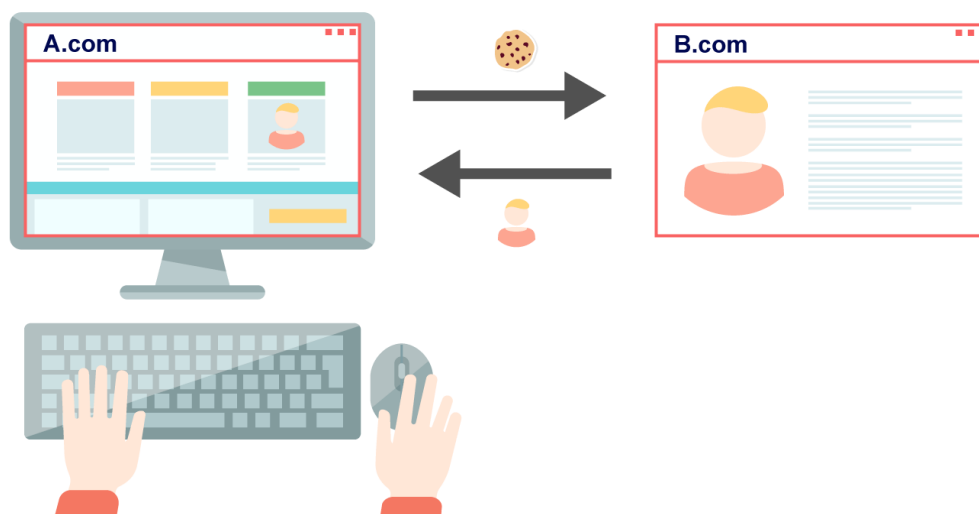
- Inyección directa de código dinámico: el software permite que las entradas sean introducidas directamente en una función que evalúa y ejecuta dinámicamente la entrada como código, generalmente en el mismo lenguaje del código. Un ejemplo son las inyecciones SQL, esta sucede cuando se inserta un trozo de código SQL dentro de otro código SQL con el fin de modificar su comportamiento, haciendo que ejecute el código malicioso en la base de datos. En el siguiente gráfico se muestra como se inyecta código SQL al realizar el alta de un usuario, en el campo clave se teclea una cadena que cierra la clave y con ; separa de otra orden sql que cambia la clave del administrador.

En el campo clave del formulario de alta de usuario introduce la inyección SQL (cierra instrucción con la comilla y el ; para ejecutar otra orden SQL que cambia la clave del administrador). La siguiente vez podrá entrar con la cuenta del administrador



- Revelación/Filtrado de información: Un filtrado o escape de información puede ser intencionado o no intencionado. En este aspecto los atacantes pueden aprovechar esta vulnerabilidad para descubrir el directorio de instalación de una aplicación, la visualización de mensajes privados, etc. La severidad de esta vulnerabilidad depende del tipo de información que se puede filtrar.
- Gestión de credenciales: Este tipo de vulnerabilidad tiene que ver con la gestión de usuarios, contraseñas y los ficheros que almacenan este tipo de información.
- Fallo de autenticación: Esta vulnerabilidad se produce cuando la aplicación o el sistema no es capaz de autenticar al usuario, proceso, etc. correctamente.
- Falsificación de petición en sitios cruzados (CSRF): Este tipo de vulnerabilidad afecta a las aplicaciones web con una estructura de invocación predecible. El agresor puede colocar en la página cualquier código, el cual posteriormente puede servir para la ejecución de operaciones no planificadas por el creador del sitio web, por ejemplo, capturar archivos cookies sin que el usuario se percate. El tipo de ataque CSRF más popular se basa en el uso del marcador HTML ``, el cual sirve para la visualización de gráficos. En vez del marcador con la URL del archivo gráfico, el agresor pone un tag que lleva a un código JavaScript que es ejecutado en el navegador de la víctima.

El usuario visita A.com, desde A.com se solicitan recursos (imagenes, ...) a B.com, a la vez que el usuario descarga esos recursos también recibe cookies de B.com que se usarán para controlar al usuario



- Error de búfer: Un búfer es una ubicación de la memoria en una computadora o en un instrumento digital reservada para el almacenamiento temporal de información digital mientras que está esperando ser procesada. Pueden ocurrir dos tipos de errores relacionados con el búfer:
 - Desbordamiento de búfer: Un búfer se desborda cuando, de forma incontrolada, al intentar meter en él más datos de los que caben, ese exceso se vierte en zonas del sistema causando daños.
 - Agotamiento de búfer: Estado que ocurre cuando un búfer usado para comunicarse entre dos dispositivos o procesos se alimenta con datos a una velocidad más baja de la que los datos se están leyendo en ellos.
- Errores numéricos: Como desbordamientos, ocurre cuando una operación aritmética procura crear un valor numérico que sea más grande del que se puede representar dentro del espacio de almacenaje disponible.
- Error en la gestión de recursos: El sistema o software que adolece de este tipo de vulnerabilidad permite al atacante provocar un consumo excesivo en los recursos del sistema (disco, memoria y CPU).
- Error de diseño: En ocasiones los programadores bien por culpa de los entornos de trabajo o bien por su metodología de programación, cometen errores en el diseño de las aplicaciones.

Seguridad física

La seguridad informática abarca un amplio espectro con el objetivo de conseguir una protección lógica y física, y que hoy en día con la conexión global (pensemos en el Internet de las cosas) hace que los sistemas estén expuestos a muchos riesgos. Veamos los aspectos más importantes de esta seguridad física

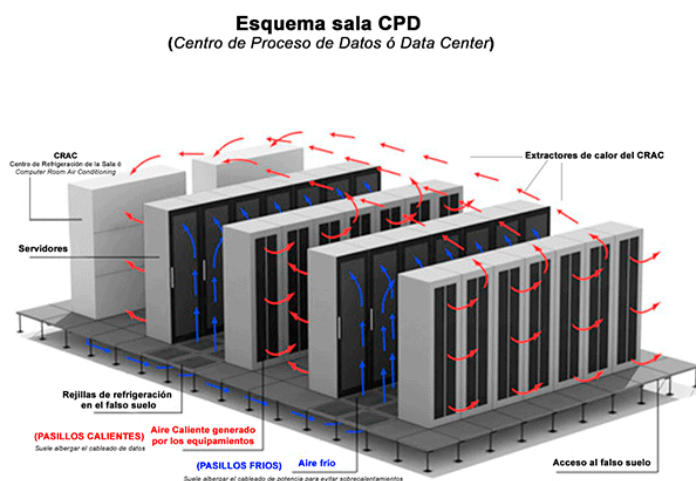
Ubicación y protección física. Condiciones ambientales

El primer paso para establecer la seguridad de un servidor o un equipo, es decidir adecuadamente dónde vamos a instalarlo. Hay centros de procesos de datos que ocupan salas enteras. Es necesario fijarse en varios factores:

- Tratamiento acústico. En general se ha de tener en cuenta que habrá equipos como los de aire acondicionado, necesarios para refrigerar los servidores, que son bastante ruidosos. Deberá instalarse el CPD en entornos donde el ruido y la vibración estén amortiguados, lejos de zonas residenciales donde puedan molestar.
- Suministro eléctrico. La alimentación de los equipos no puede estar sujeta a las fluctuaciones de la red eléctrica. Es conveniente utilizar SAIs. En el caso de los centros de procesos de datos se trata de un factor fundamental.
- Las comunicaciones. Habrá que estudiar que en la ubicación seleccionada exista acceso a comunicaciones con suficiente ancho de banda.
- Condiciones medioambientales. Construiremos el CPD en espacios donde los factores naturales no sean muy adversos, como el frío o calor.
- La seguridad del entorno: La zona en que se situé el CPD debe ser tranquila, pero no un sitio desolado. Habrá que tener en cuenta fenómenos como el vandalismo, el sabotaje y el terrorismo.
- Deben evitarse áreas con fuentes de interferencia de radiofrecuencia, tales como transmisores de radio y estaciones de televisión.
- El CPD no puede estar contiguo a maquinaria pesada o almacenes de gas inflamable o nocivo.

De modo complementario a la correcta elección de la ubicación de un CPD, es necesario un férreo control de acceso al mismo. Poniendo servicio de vigilancia, detectores de metales, sistemas biométricos de acceso, etc.

Los equipos de un CPD disipan mucha energía calorífica y hay que refrigerarlos adecuadamente.



Sistemas de alimentación ininterrumpida (SAI)



Un SAI o sistema de alimentación ininterrumpida es un dispositivo electrónico que permite proteger a los equipos frente a los picos o caídas de la tensión eléctrica. De esta manera, se dispone de mayor estabilidad

frente a los cambios del suministro eléctrico y de una fuente de corriente alternativa cuando se produce un corte de luz. A los SAI se les conoce como UPS (Uninterruptible Power Supply en inglés). Las características de un SAI son las siguientes:

- Potencia. Se mide en vatios o voltio amperios. De ella depende el número de ordenadores que podemos conectar al SAI.
- Autonomía. Es el tiempo que nos permite trabajar desde que se produce el corte de suministro.
- Regulador de voltaje. Evita que los picos de tensión que se producen en la línea afecten a los equipos. Estabilizan la corriente eléctrica.
- Otros conectores auxiliares. Algunos incorporan conectores para la línea telefónica, el modem, router... y así proteger los dispositivos que hacen posible la comunicación.

Seguridad lógica

La seguridad lógica trata de impedir los daños que se producen por las amenazas lógicas tales como impedir el acceso no autorizado, evitar la pérdida de datos, etc.

Políticas de almacenamiento

Las copias de seguridad de los datos son copias de información que se deben guardar en un lugar diferente al original para evitar que daños como incendios o similares destruyan todas las copias.

Los centros de respaldo son ubicaciones donde se guardan las copias de seguridad. Estas ubicaciones deben estar protegidas de la misma manera que los CPD: con controles de acceso, detección de fuego, etc.



Las copias de seguridad deben realizarse de todos los archivos que sean difíciles o imposibles de reemplazar o recuperar. En principio no hace falta hacer una copia de seguridad de los sistemas operativos o software pues suele ser fácil la reinstalación.

Debemos evitar:

- Guardar la copia en el mismo soporte que los datos originales (si se daña el soporte perdemos todos los datos)
- Evitar almacenarlas en el mismo lugar como comentamos anteriormente
- Reemplazar una copia sobrescribiendo copias antiguas, si la pérdida de información se produce entre estas 2 copias la nueva copia destruirá los datos.

Hay muchas herramientas que permiten hacer copias de seguridad de los datos, protegiéndolos de posibles pérdidas parciales o totales, automatizando el proceso de realización de las copias e incluso comprimiendo y cifrando las copias.

Las copias de seguridad remotas o en la nube son servicios que nos proporcionan proveedores para realizar de forma automática y a través de internet el proceso de salvaguardar los datos de nuestro sistema.


Toda política de seguridad de una empresa debe contemplar los siguientes puntos:

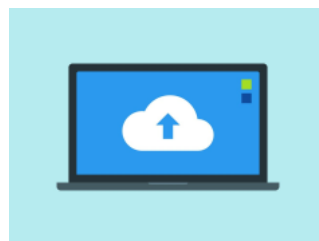
- Persona responsable: Habrá que determinar la persona o personas responsables de realizar y mantener ordenadas las copias de seguridad.
- Datos a salvaguardar: Debemos analizar los datos susceptibles de ser salvaguardados en copias de seguridad.
- Tipo de copia a realizar: Debemos determinar si realizamos copias completas, diferenciales o incrementales. Si el volumen de información es muy elevado no podemos hacer copias completas de forma frecuente (a diario) porque nos llevaría mucho tiempo. Si la información que se modifica o añade es muy elevada sería mejor optar por las incrementales. En caso contrario, por las diferenciales.
- Frecuencia de la copia: Las copias completas se realizan en intervalos de tiempo más amplios. Las copias incrementales o diferenciales suelen realizarse a diario, en empresas normales.
- Ventana de backup: Será la franja horaria en la que se deben realizar las copias de seguridad.
- Tipo de soporte: Discos magnéticos externos, discos SSD, unidades de red,...
- Ubicación de las copias de seguridad: Lugar alejado al del origen.

[Guía sobre copias de seguridad del INCIBE](#)

Medios de almacenamiento

Dentro de los medios de almacenamiento podemos encontrar:

- DAS (Direct-Attached Storage) es el método de almacenamiento tradicional y consiste en conectar el dispositivo de almacenamiento directamente al ordenador o servidor. Su desventaja es que no suele ser un almacenamiento compartido por otros equipos.
- NAS (Network Attached Storage) son dispositivos de almacenamiento que están conectados a la red local directamente, sin la necesidad de estar asociados a ningún pc concreto. Están encendidos permanentemente, y permiten el acceso a cualquier equipo de la red. Se accede a través de protocolo TCP/IP. Son discos duros de red con una dirección IP propia. Su utilización es aconsejable en empresas pequeñas con no demasiado volumen de información
-  SAN (Storage Area Network) es una red de almacenamiento, está pensada para almacenar servidores de archivos, discos de almacenamiento NAS, etc... utilizando tecnologías de comunicación de alta velocidad como la fibra óptica (que alcanzan hasta 8 Gb/s). Las SAN al ser construidas con fibra óptica heredan los beneficios de ésta, por ejemplo, las SAN pueden tener dispositivos de almacenamiento con una separación de hasta 10 Km sin repetidores.
- Clustered NAS es una versión mejorada del NAS y se basa en la disponibilidad de varios servidores que comparten los mismos volúmenes, permitiendo un mejor reparto de la carga de trabajo y el añadido de disponer de más interfaces de comunicación Ethernet.

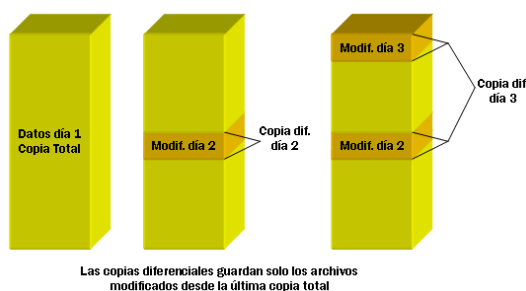


- Cloud o en la nube es un almacenamiento al que se accede mediante una conexión de Internet o IP a servidores en remoto, fuera de la red local.
- SDS (Almacenamiento Definido por Software): permite abstraer recursos de almacenamiento hardware subyacente para lograr más flexibilidad, eficiencia y escalabilidad mediante software o programación de los recursos de almacenamiento. Utilizados para datos no estructurados, sistemas de archivos distribuidos..., utilizado en virtualización, cloud...

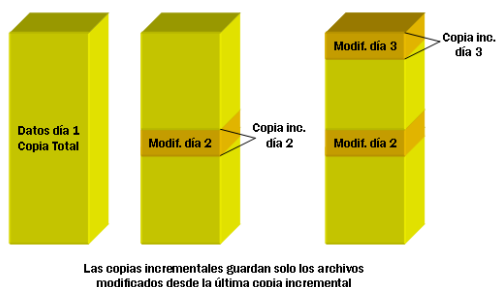
Tipos de copias de seguridad

Dependiendo de la cantidad de ficheros que se almacenan en el momento de realizar la copia, podemos distinguir tres clases de copias de seguridad:

- Completa: Como su nombre indica, se realiza una copia de todos los archivos y directorios seleccionados. Si el volumen de información es elevado (cientos de gigabytes) no podemos realizar una copia completa a diario, por la cantidad de tiempo que conlleva.
- Diferencial: Se utiliza días después de haber realizado una copia completa. Se copian sólo los nuevos archivos y archivos modificados desde el día que se hizo la copia completa.



- Incremental: Este tipo de copia se parece mucho a la anterior, a diferencia de que sólo almacena los archivos creados y modificados después de la última copia incremental realizada.



Recuperación del sistema

Desgraciadamente el sistema operativo también falla o funciona de manera imprevisible, una solución será realizar una imagen del sistema operativo recién instalado para así restablecer su correcto funcionamiento lo más rápidamente posible y evitar su instalación desde cero.

Pero antes de esto, podemos intentar restaurar el sistema operativo del equipo al estado en el que se encontraba antes de realizar la acción que produjo la avería. Para ello debemos crear y guardar puntos de restauración. Estos puntos almacenan los archivos más importantes del sistema.

El punto de restauración almacena entre otros: El registro de Windows, los archivos del sistema, cuentas y contraseñas de usuarios, drivers de los dispositivos, configuración de las aplicaciones.

Otra forma de recuperar el equipo es mediante la restauración de imágenes del disco, para ello debemos realizar previamente una clonación del disco, una copia idéntica de todos los archivos que contiene a otro disco duro.

Recuperación de datos y borrado seguro

Al igual que podemos recuperar el sistema se pueden recuperar datos mediante restauración de copias de seguridad, pero si no disponemos de una copia reciente la solución pasa por recuperar los datos borrados puesto que cuando procedemos a borrar datos realmente lo que se realiza es una marcación como zona libre en el sistema de almacenamiento del lugar que ocupaban esos datos

El primer paso es ir directamente a la papelera del sistema e intentar recuperarlos, si no es posible podemos recurrir a aplicaciones de recuperación. Se puede pensar que un simple formateo del disco duro impedirá que los datos almacenados en el mismo puedan ser recuperados. Sin embargo, hay aplicaciones que permiten deshacer el formateo de una unidad existiendo incluso métodos para recuperar los datos de los discos, aunque estos hayan sido sobrescritos.

Pero esto es un arma de doble filo porque es posible que deseemos borrarlos y que no se puedan recuperar porque se trate de datos sensible, en tal caso, se deben sobrescribir los datos siguiendo un método (patrón de borrado) que no permita su recuperación de modo alguno.

Para tal fin, es necesario realizar diversas pasadas de escritura sobre cada uno de los sectores donde se almacena la información. Para simplificar la tarea, lo más sencillo es utilizar alguna aplicación especializada que permita eliminar la información de forma sencilla

Criptografía

La criptografía (del griego “oculto” y “escribir”, literalmente “escritura oculta”) es el arte o ciencia de cifrar y descifrar información mediante técnicas especiales y se emplea frecuentemente para permitir un intercambio de mensajes que solo puedan ser leídos por personas a las que van dirigidos y que poseen medios para descifrarlos.

La criptografía se considera una rama de las Matemáticas y en la actualidad de la Informática y la Telemática, que hace uso de métodos y técnicas matemáticas con el objetivo principal de cifrar un mensaje o archivo por medio de un algoritmo, usando una o más claves.

En la terminología de criptografía, encontramos los siguientes aspectos:

- La información original que debe protegerse se denomina texto en claro o texto plano.
- El cifrado es el proceso de convertir el texto plano en un texto ilegible, denominado texto cifrado o criptograma.
- Los algoritmos de cifrado se dividen en dos grandes tipos:

- De cifrado en bloque: dividen el texto origen en bloques de bits de un tamaño fijo y los cifran de manera independiente.
- De cifrado de flujo: el cifrado se realiza bit a bit, byte a byte o carácter a carácter.
- Las dos técnicas más sencillas de cifrado, en la criptografía clásica, son:
 - La sustitución: supone el cambio de significado de los elementos básicos del mensaje, las letras, los dígitos o los símbolos.
 - La transposición: supone una reordenación de los mismos pero los elementos básicos no se modifican en sí mismos.
- El descifrado es el proceso inverso que recupera el texto plano a partir del criptograma y la clave.

Según el principio de Kerchoff la fortaleza de un sistema o algoritmo de cifrado debe recaer en la clave y no en el algoritmo, cuyos principios de funcionamiento son conocidos normalmente, en caso de no conocer la clave no podremos descifrar el mensaje.

Criptografía de clave simétrica

La criptografía simétrica es un método criptográfico en el cual se usa una misma clave para cifrar y descifrar mensajes. Las dos partes que se comunican han de ponerse de acuerdo de antemano sobre la clave a usar. Una vez ambas tienen acceso a esta clave, el remitente cifra un mensaje usándola, lo envía al destinatario y éste lo descifra con la misma.



Un buen sistema de cifrado pone toda la seguridad en la clave y ninguna en el algoritmo. Dado que toda la seguridad está en la clave, es importante que sea muy difícil adivinar el tipo de clave. Esto quiere decir que el abanico de claves posibles, o sea, el espacio de posibles claves debe ser amplio. Esto lo posibilita la longitud y el conjunto de caracteres que emplee. Algunos ejemplos de algoritmos de cifrado simétrico son:

- El algoritmo de cifrado DES usa una clave de 56 bits, lo que significa que hay 2^{56} claves posibles. Esto representa un número muy alto de claves, pero un ordenador genérico puede comprobar el conjunto posible de claves en cuestión de horas.
- Algoritmos de cifrado como 3DES, Blowfish e IDEA usan claves de 128 bits, lo que significa que existen 2^{128} claves posibles. La mayoría de las tarjetas de crédito y otros medios de pago electrónicos tienen como estándar el algoritmo 3DES.

- Otros algoritmos de cifrado muy usados son RC5 y AES, Advanced Encryption Standard, también conocido como Rijndael, estándar de cifrado por el gobierno de Estados Unidos.

Los principales problemas de los sistemas de cifrado simétrico son:

- El intercambio de claves. Una vez que el remitente y el destinatario hayan intercambiado las claves pueden usarlas para comunicarse con seguridad, pero ¿qué canal de comunicación seguro han usado para transmitirse las claves? Sería mucho más fácil para un atacante interceptar una clave que probar las posibles combinaciones del espacio de claves.
- El número de claves que se necesitan. Si tenemos un número n de personas que necesitan comunicarse entre sí, se necesitan $n/2$ claves diferentes para cada pareja de personas que tengan que comunicarse de modo privado. Esto puede funcionar con un grupo reducido de personas, pero sería imposible llevarlo a cabo con grupos más grandes.

Para solucionar estos problemas se mejora la seguridad de los sistemas, mediante la criptografía asimétrica y a criptografía híbrida.

Criptografía de clave asimétrica

En este caso, cada usuario del sistema criptográfico ha de poseer una pareja de claves:

- Clave privada: será custodiada por su propietario y no se dará a conocer a ningún otro.
- Clave pública: será conocida por todos los usuarios.

Esta pareja de claves es complementaria: lo que cifra una solo lo puede descifrar la otra y viceversa. Estas claves se obtienen mediante algoritmos y funciones matemáticas complejas de forma que por razones de tiempo de cómputo, es imposible conocer una clave a partir de la otra.



Ana escribe un mensaje (1), lo cifra con la clave pública de David (2), lo envía (3), David lo descifra con su clave privada (4) y, lee el mensaje (5).

Lo correcto es que la clave privada no salga nunca de nuestro poder, con la clave pública se cifra un mensaje o verifica una firma y con la clave privada se descifra un mensaje o se realiza una firma.

Los sistemas de cifrado de clave pública se basan en funciones resumen o funciones hash de un solo sentido que aprovechan propiedades particulares, por ejemplo, de los números primos. Una función de un solo sentido es aquella cuya computación es fácil, mientras que su inversión resulta extremadamente difícil.

Una **función hash** es un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija. Independientemente de la longitud de los datos de entrada, el valor hash de salida tendrá

siempre la misma longitud y, además, si cambia un solo carácter de los datos de entrada se produce un hash diferente.

Una función hash tiene dos usos muy típicos:

- Almacenar las claves de usuario, no se almacena la clave si no que se almacena su hash esto permite que aunque se acceda a la base de datos de claves (mejor dicho de hash de claves) es muy difícil averiguar la clave del usuario. Para validar al usuario cada vez que este teclea una clave se le aplica la función hash y se compara con el hash almacenado en la base de datos.
- Validar archivos, si conocemos el hash del archivo nadie puede hacer cambios en el archivo sin que se produzca un hash diferente. Es en lo que se basan los Código Seguro de Verificación (CSV)

Algunos de los algoritmos empleados como funciones resumen o hash son MD5 y SHA.

Dentro de los algoritmos de clave asimétrica tenemos:

- Algoritmo RSA, Sistema criptográfico de clave pública diseñado por Rives, Shamir y Adleman en 1979. No vulnerado aún pero es considerado un algoritmo de cifrado/descifrado lento.
- Algoritmo Elgamal, Descrito por Taher Elgamal en 1984, es el algoritmo usado en las aplicaciones de GPG. Tampoco ha sido vulnerado, y también se considera lento.
- Algoritmo ECC, Algoritmo Elliptic Curve cryptography, es también un algoritmo de clave asimétrica. Fue creado por Neal Koblitz y Victor Miller en 1985. No ha sido vulnerado, utiliza claves de cifrado más cortas para lograr un nivel de seguridad similar, por lo que lo convierte en un algoritmo más rápido.

Criptografía híbrida

El uso de claves asimétricas ralentiza el proceso de cifrado. Para solventar dicho inconveniente, el procedimiento que suele seguirse para realizar el cifrado de un mensaje es utilizar un algoritmo de clave pública, más seguro, tan solo empleado para el cifrado en el envío de una pequeña cantidad de información: por ejemplo una clave asimétrica, junto a uno de clave simétrica, para el cifrado del mensaje, reduciendo de esta forma el coste computacional.

Monedas digitales

Son medios de intercambio de dinero en forma digital, no existen billetes ni monedas físicas, dentro de las monedas digitales el caso más conocido son las criptomonedas que utilizan la criptografía para asegurar, verificar las transacciones y crear nuevas unidades, también se caracterizan porque tienen un control descentralizado a través de redes P2P.

Esencialmente, las criptomonedas son entradas limitadas en una base de datos de bloques (blockchain, los datos se guardan en bloques y cada nuevo bloque contiene un hash del bloque anterior por lo no se pueden realizar cambios, a no ser que se hagan en cadena). Existen miles de criptomonedas, la más popular es bitcoin.

Cada transacción es un archivo que consta de las claves públicas del remitente y el destinatario y la cantidad de monedas transferidas. Las claves son guardadas en las carteras o wallets,

habrá claves públicas de otros usuarios y la clave privada del propietario. La transacción también debe ser firmada por el remitente con su clave privada y finalmente es transmitida a la red una vez es confirmada por sus usuarios dedicados a esta tarea, denominados “mineros”. Dentro de una red de criptomonedas, solo los mineros pueden confirmar las transacciones resolviendo cálculos criptográficos. Toman transacciones, las marcan como legítimas y las difunden a través de la red. Después, cada nodo de la red lo agrega a su base de datos (blockchain). Una vez que se confirma la transacción, se vuelve irrefutable e irreversible y un minero recibe una recompensa económica en bitcoins.

Esteganografía

Es la técnica de ocultar información dentro de otra información, en vez de cifrar el mensaje lo que se hace es ocultarlo dentro de otra información. La esteganografía se puede incorporar a las tecnologías informáticas de diferentes formas como ocultar texto en una imagen, vídeo o canción, ya sea por diversión, para proteger un archivo de la copia ilegal o para enviar información oculta.

La esteganografía puede ser utilizada para proteger comunicaciones ocultando la información que se envía desde código spyware o para ocultar código maligno dentro de imágenes o similares.

Sistemas de identificación

Los métodos de autenticación, en nuestro caso, son los mecanismos que una máquina tiene para comprobar que el usuario que intenta acceder es quien dice ser. Hay diferentes medios para identificarse algún dato conocido (clave, fecha nacimiento,...), alguna posesión (tarjeta), algún rasgo (huellas, iris,...). También se pueden usar métodos combinados (tarjeta + pin).

En la mayoría de los equipos informáticos, la autenticación de los usuarios se realiza introduciendo un nombre y una contraseña. Cada usuario tiene asignado un identificador y una clave, que permitirán comprobar la identidad del mismo en el momento de la autenticación.

Los sistemas de control de acceso protegidos con contraseña suelen ser un punto crítico de la seguridad y, por ello, suelen recibir distintos tipos de ataques. Los más comunes son:

- Ataques de fuerza bruta: Se intenta recuperar una clave probando todas las combinaciones posibles hasta encontrar aquella que permite el acceso. Cuanto más corta, más sencilla de obtener probando combinaciones.
- Ataque de diccionario: Intenta averiguar una clave probando todas las palabras de un diccionario o conjunto de palabras comunes. Este tipo de ataque suele ser más eficiente que un ataque de fuerza bruta, ya que muchos usuarios suelen utilizar una palabra existente en su lengua como contraseña para que la clave sea fácil de recordar, lo cual no es una práctica recomendable.
- Ataque según análisis estadístico: Se intenta averiguar una clave por patrones de contraseña típicos.

Como es lógico pensar, la seguridad del sistema va a estar fuertemente relacionada con la buena elección de la contraseña y la confidencialidad de la misma. A continuación, vamos a estudiar las características que debe cumplir una buena contraseña:

- No deben estar formadas por palabras que encontremos en diccionarios.
- No deben usarse sólo letras mayúsculas o minúsculas.
- No deben estar formadas exclusivamente por números por el mismo motivo.
- No debemos utilizar información personal: nombre de nuestros familiares, fecha de nacimiento, número de teléfono, etc.
- No debemos repetir los mismos caracteres en la misma contraseña.
- No debemos escribir la contraseña en ningún sitio, ni en papel ni en ordenador.
- No debemos enviarlo en ningún correo electrónico que nos la solicite.
- Debemos limitar el número de intentos fallidos.
- Debemos cambiar las contraseñas de acceso dadas por defecto por los fabricantes.
- No debemos utilizar la misma contraseña en las distintas máquinas o sistemas.
- Las contraseñas deben caducar y exigir que se cambien cada cierto tiempo.
- No debemos permitir que las aplicaciones recuerden las contraseñas.

Sistemas biométricos

Los sistemas biométricos, se utilizan para **autenticar a los usuarios a través de sus rasgos físicos o conductas**. Estos sistemas se están popularizando en la actualidad; podemos encontrar portátiles que nos obligan a autenticarnos para acceder a su sistema operativo a través de la detección de la huella digital. Otro caso similar nos lo encontramos en Disney World. La identificación de los usuarios que poseen entrada válida para varios días se realiza mediante sistemas biométricos; de esta manera se evita que un grupo de amigos saquen entradas para varios días aprovechando el descuento y que posteriormente accedan al parque en distintas días repartidos en pequeños grupos.

El funcionamiento del sistema biométrico se compone de dos módulos, el de inscripción y el de identificación/reconocimiento.

- Módulo de inscripción: mediante sensores biométricos, se lee y extrae la característica que identifica al usuario, almacenando el patrón en una base de datos. En el caso del acceso a una empresa, tendríamos que almacenar el patrón de todos los empleados que están autorizados a acceder a la misma.
- El módulo de identificación o reconocimiento: lee y extrae la característica que reconoce al usuario. Ese patrón es comparado con los que se tienen almacenados en la base de datos y se devuelve la decisión sobre la identidad del usuario.



Los tipos de sistemas biométricos más populares son:

- Verificaciones anatómicas:
 - Mano: huellas dactilares, geometría, venas.
 - Rostro: geometría.
 - Patrones oculares: retina, iris.
- Verificación del comportamiento:
 - Timbre de la voz.
 - Escritura: escritura manual de un texto predefinido, firma del usuario.
 - Longitud y cadencia del paso.

Firma digital

Una de las principales ventajas de la criptografía de clave pública es que ofrece un método para el desarrollo de firmas digitales.

La firma digital permite al receptor de un mensaje verificar la autenticidad del origen de la información, así como verificar que dicha información no ha sido modificada desde su generación. De este modo, la firma digital ofrece el soporte para la autenticación e integridad de los datos, así como para el no repudio en origen, ya que la persona que origina el mensaje firmado digitalmente no puede argumentar que no lo hizo.

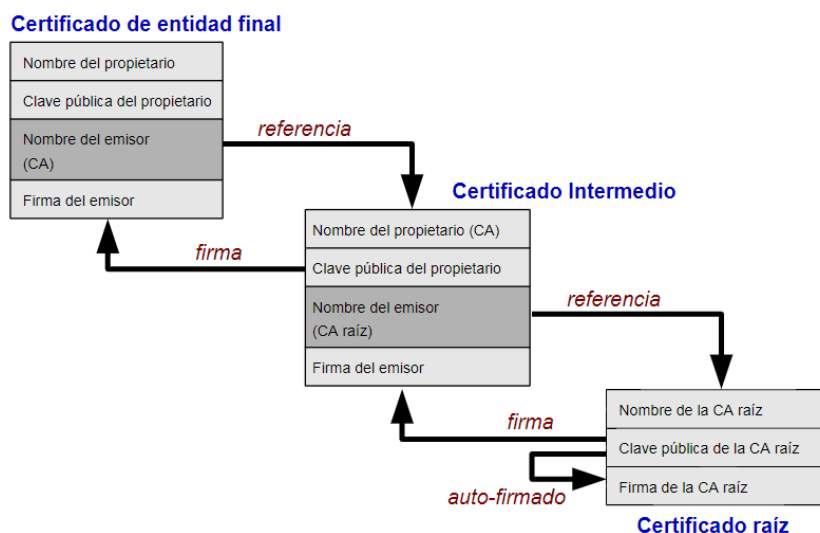
Una firma digital está destinada al mismo propósito que una firma manuscrita. Sin embargo, una firma manuscrita es sencilla de falsificar mientras que la digital es imposible mientras no se descubra la clave privada del firmante.

La firma digital es un cifrado del mensaje que se está firmando pero utilizando la clave privada en lugar de la pública. Recordemos, el propietario del certificado digital, firma con su clave privada y el receptor verifica con la clave pública y; el propietario del certificado digital descifra los mensajes enviados por un tercero y que están cifrados con su clave pública.

Sin embargo, como ya se ha comentado, el principal inconveniente de los algoritmos de clave pública es su lentitud que, además, crece con el tamaño del mensaje a cifrar. Para evitar este problema, la firma digital es el resultado de cifrar con clave privada el resumen de los datos a firmar, haciendo uso de funciones resumen o hash.

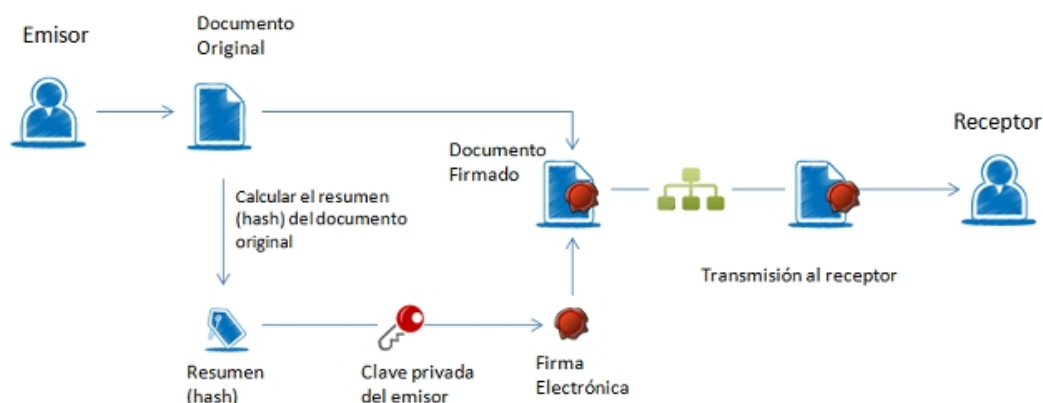
Actualmente está muy extendido el uso de certificados digitales. En general un certificado digital es un archivo que puede emplear un software para firmar digitalmente archivos y mensajes por ejemplo de correo electrónico, en los cuales puede verificarse la identidad del firmante.

Como ejemplo encontramos los certificados digitales que identifican a personas u organizaciones, y que contienen información sobre una persona o entidad. Estos certificados son emitidos por una autoridad certificadora. Verificando el emisor (la autoridad certificadora CA) y los demás certificados involucrados en la cadena de confianza se puede asegurar si el certificado lo ha emitido dicha entidad y de este modo validarlo.



De Yanpas - Trabajo propio, CC BY-SA 4.0, <https://commons.wikimedia.org/w/index.php?curid=46369922>

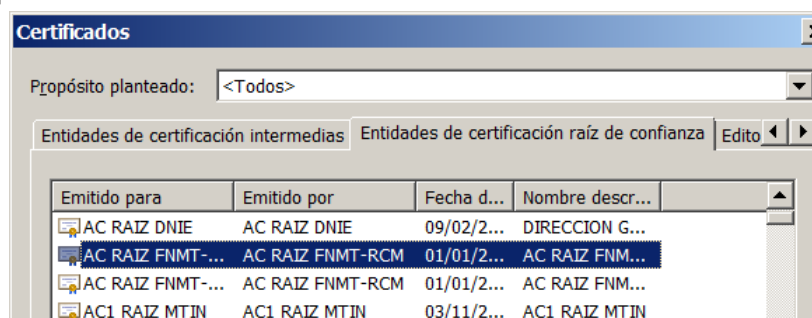
La autoridad certificadora es un tipo particular de Prestador de Servicios de Certificación que legitima ante los terceros, se trata de una cadena de confianza jerárquico, las Autoridades de Certificación disponen de un certificado conocido como Certificado Raíz (Root CA), y como su nombre indica es el certificado que validará todos y cada uno de los certificados emitidos por la CA; sin embargo, este certificado no es el que firmará los certificados de suscriptor (o certificados finales), sino se empleará únicamente para firmar los denominados Certificados Subordinados (Sub-CA), y estos últimos firmarán los certificados de suscriptor (o finales). Se muestra un diagrama ejemplo del modelo jerárquico para ilustrar el funcionamiento de la cadena de confianza de certificados. En España, tenemos a la [FNMT](#) (Fábrica Nacional de moneda y timbre), a nivel de empresas privadas certificadoras tenemos, por ejemplo, [Verisign](#)



El proceso paso a paso en un envío de Emisor a Receptor sería el siguiente:

- El emisor crea un nuevo mensaje.
- El emisor obtiene mediante una función hash un resumen del mensaje
- El emisor cifra el resumen usando su clave privada y obtiene el resumen cifrado
- El emisor envía: el mensaje original (sin cifrar) + resumen cifrado + certificado digital (que contiene clave pública del emisor + datos personales). Este certificado digital está cifrado por la entidad emisora del certificado (CA).

- El receptor recibe el mensaje
- El receptor descifra el certificado digital del emisor utilizando el certificado raíz de la entidad emisora que se encuentra en el almacén de certificados de su equipo:



- Una vez ha descifrado el certificado digital del emisor, el receptor accede a la clave pública para descifrar el resumen cifrado por el emisor
- El receptor usa la misma función hash que el emisor y comprueba que el resumen coincide con el descifrado anteriormente. Si coincide todo es correcto, el mensaje puede ser considerado válido.

Con este sistema conseguimos:

- Autenticación: La firma del mensaje es equivalente a la firma física de un documento.
- Integridad: El mensaje no podrá ser modificado, si se ha modificado la función hash da un resultado diferente.
- No repudio en el origen: El emisor no puede negar haber enviado el mensaje.

El formato estándar de certificados digitales es X.509 y su distribución es posible realizarla:

- Con clave privada (suele tener extensión *.pfx en Internet Explorer o *.p12 en Firefox) más seguro y destinado a un uso privado de exportación e importación posterior como método de copia de seguridad.
- Solo con clave pública (suele ser de extensión *.cer o *.crt), destinado a la distribución no segura, para que otras entidades o usuarios tan solo puedan verificar la identidad, en los archivos o mensajes cifrados.

Entre otras aplicaciones de los certificados digitales y el DNIE encontramos, realizar compras y comunicaciones seguras, como trámites con la banca online, con la administración pública (hacienda, seguridad social, etc.) a través de Internet, etc.

Auditorías de Seguridad Informática

Una auditoría de seguridad informática o auditoría de seguridad de sistemas de información (SI) es el estudio que comprende el análisis y gestión de sistemas llevado a cabo por profesionales generalmente por Ingenieros Informáticos para identificar, enumerar y posteriormente describir las diversas vulnerabilidades que pudieran presentarse en una revisión exhaustiva de las estaciones de trabajo, redes de comunicaciones o servidores.

Una vez obtenidos los resultados, se detallan, archivan y reportan a los responsables quienes deberán establecer medidas preventivas de refuerzo y/o corrección siguiendo siempre un proceso secuencial que permita a los administradores mejorar la seguridad de sus sistemas aprendiendo de los errores cometidos con anterioridad.

Las auditorías de seguridad de SI permiten conocer en el momento de su realización cuál es la situación exacta de sus activos de información en cuanto a protección, control y medidas de seguridad.

Los servicios de auditorías pueden ser de distintos tipos:

- Auditoría de seguridad interna. En este tipo de auditoría se contrasta el nivel de seguridad y privacidad de las redes locales y corporativas de carácter interno.
- Auditoría de seguridad perimetral. En este tipo de análisis, el perímetro de la red local o corporativa es estudiado y se analiza el grado de seguridad que ofrece en las entradas exteriores.
- Test de intrusión. Es un método de auditoría mediante el cual se intenta acceder a los sistemas, para comprobar el nivel de resistencia a la intrusión no deseada. Es un complemento fundamental para la auditoría perimetral.
- Análisis forense. El análisis forense es una metodología de estudio ideal para el análisis posterior de incidentes, mediante el cual se trata de reconstruir cómo se ha penetrado en el sistema, a la par que se valoran los daños ocasionados. Si los daños han provocado la inoperabilidad del sistema, el análisis se denomina análisis postmortem.
- Auditoría de páginas web. Entendida como el análisis externo de la web, comprobando vulnerabilidades como la inyección de código sql, Verificación de existencia y anulación de posibilidades de Cross Site Scripting (XSS), etc.
- Auditoría de código de aplicaciones. Análisis del código tanto de aplicaciones páginas web como de cualquier tipo de aplicación, independientemente del lenguaje empleado.

Realizar auditorías con cierta frecuencia asegura la integridad de los controles de seguridad aplicados a los sistemas de información. Acciones como el constante cambio en las configuraciones, la instalación de parches, actualización del software y la adquisición de nuevo hardware hacen necesario que los sistemas estén continuamente verificados mediante auditoría.

Análisis forense



El análisis forense informático es un recurso imprescindible en la seguridad informática que permite conocer donde se ha producido el problema y quien está detrás.

Un análisis forense está estructurado en una serie de fases que están orientadas a evidenciar el origen de los problemas. Las principales son:

- Fase de protección: Es la primera medida que se aplica y el objetivo es impedir que ninguna persona externa pueda alterar el sistema informático de la víctima una vez que empieza la investigación.
- Fase de identificación: A continuación, el equipo debe recolectar una serie de pruebas o indicios que nos ayudarán a constatar las irregularidades que se han producido dentro del sistema.
- Recolección de datos: Es probablemente la fase más delicada de todo el proceso ya que puede originar una alteración o modificación de las evidencias delictivas. Si esto ocurre las pruebas recolectadas pueden ser invalidadas dentro de un proceso judicial.
- Análisis: Una vez recolectada la información relevante se procede a un análisis de la misma. En este punto del proceso se inicia un estudio de todos aquellos ficheros que pueden albergar cualquier información ya eliminada, así como registros, logs y accesos al sistema de la víctima, etc.
- Informe de resultados: Una vez que se ha recopilado la información y se han relacionado procesos e indicios llega el momento de aglutinar toda la información. Cuando se finaliza un análisis forense digital resulta imprescindible redactar un informe de tipo de pericial donde se incluyen las conclusiones finales. El documento debe ser legible claro y preciso para los tribunales judiciales.

Hoy es posible acceder a todo tipo de herramientas especializadas en el análisis de dispositivos de todo tipo. Estas herramientas son capaces de focalizar su acción en una capa determinada de la infraestructura digital que ha sido afectada dentro de un sistema.

A pesar de que existe una gran cantidad de recursos específicos, los datos de la red no son totalmente confiables. Por ello es necesario implementar sistemas realmente eficaces y capaces de perseguir el cibercrimen de una forma precisa.